GROUPE "ARTICLE 29" SUR LA PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL

5035/01/FR/Final
WP 56

Document de travail : Application internationale du droit de l'UE en matière de protection des données au traitement des données à caractère personnel sur Internet par des sites web établis en dehors de l'UE

Adopté le 30 mai 2002

Le groupe, institué par l'article 29 de la directive 95/46/CE, est l'organe communautaire indépendant et à caractère consultatif sur la protection des données et de la vie privée. Ses missions sont définies à l'article 30 de la directive 95/46/CE et à l'article 14 de la directive 97/66/CE. Le secrétariat est assuré par:

La Commission européenne, DG Marché intérieur, Fonctionnement et impact du Marché intérieur. Coordination. Protection des données.
B-1049 Bruxelles - Belgique - Bureau : C100-6/136
Adresse Internet: http://europa.eu.int/comm/privacy

LE GROUPE DE TRAVAIL PROTECTION DES PERSONNES PHYSIQUES A L'EGARD DU TRAITEMENT DES DONNEES A CARACTERE PERSONNEL

institué par la directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995[1],

vu les articles 29 et 30 paragraphes 1 (a) et 3 de la directive,

vu le règlement de procédure du groupe de travail et en particulier les articles 12 et 14,

a adopté le présent document de travail :

1. Introduction

L'objectif du présent document est d'aborder la question de l'application internationale du droit de l'UE en matière de protection des données au traitement (collecte en particulier) des données à caractère personnel par des sites web établis en dehors de l'Union européenne[2]. L'objectif de ce document de travail est de constituer un outil de référence pour les responsables du traitement et leurs conseillers lors de l'examen des cas impliquant le traitement de données à caractère personnel sur Internet par des sites web établis en dehors de l'Union européenne. En raison de la complexité élevée du domaine et du dynamisme de l'environnement Internet, ce document ne prétend pas proposer de solution définitive pour chaque cas de figure possible en rapport avec la question.

Dans son document de travail « La vie privée sur l'Internet »[3], le groupe de travail « article 29 » sur la protection des données a identifié un besoin évident de spécifier l'application concrète de la règle sur le droit applicable de la directive générale en matière de protection des données (article 4 paragraphe 1 (c))[4], en particulier pour le traitement en ligne de données à caractère personnel par un responsable établi en dehors du territoire communautaire. Les autorités nationales de contrôle de la protection des données sont régulièrement invitées à conseiller en ces matières les sociétés et les particuliers.

La nécessité de déterminer si le droit national s'applique aux situations qui présentent des liens vers plusieurs autres pays n'est pas spécifique à la protection des données, ni à

---

[1] Journal officiel n° L 281 du 23 novembre 1995, p. 31, disponible à l'adresse : http://europa.eu.int/comm/internal_market/en/dataprot/index.htm

[2] La directive 95/46/CE relative à la protection des données a également été mise en œuvre au sein de l'Espace économique européen (EEE). La référence à l'Union européenne dans le présent document doit être comprise comme une référence à l'EEE.

[3] « Le respect de la vie privée sur Internet – Une approche européenne intégrée sur la protection des données en ligne », WP 37, 21 novembre 2000

[4] La directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données
J.O. n° L 281 du 23 novembre 1995, p. 31 à 50., disponible à l'adresse :
http://europa.eu.int/eur-lex/fr/lif/dat/1995/fr_395L0046.html

l'Internet, ni à l'Union européenne. C'est une question générale de droit international qui se présente dans les situations en ligne et hors ligne, pour lesquelles un ou plusieurs éléments présents concernent plus d'un pays. Une décision est nécessaire quant à savoir si le droit national doit être appliqué à ces situations avant de pouvoir dégager une solution en substance.

Ces décisions impliquent la prise en compte d'un certain nombre de facteurs. Tout d'abord, la préoccupation d'un État donné est de protéger les droits et les intérêts de ses citoyens, résidents, industries et autres électeurs reconnus par le droit national. Dans de nombreux pays, le droit pénal (contrairement aux lois accordant des droits et des libertés) exige l'application la plus large et des effets au niveau international. Des affaires célèbres – Yahoo![5] ou CompuServe[6] par exemple – montrent comment les tribunaux appliquent le droit pénal national pour interdire l'accès à des contenus pornographiques ou racistes sur des serveurs Internet étrangers. Une récente décision de la Cour suprême allemande sur des affaires pénales a condamné un éditeur du « Auschwitz Lüge » (dénégation de l'existence d'Auschwitz) sur un site web australien bien qu'il n'ait pas été prouvé que ce site avait réellement été consulté à partir de l'Allemagne[7]. Selon la Cour de justice, dans le contexte de ce délit particulier, le fait que le contenu Internet « puisse » avoir un effet défavorable sur l'ordre public en Allemagne suffit ; il n'est pas nécessaire qu'il se soit effectivement produit.

Une telle application au niveau international de règles protectrices exprime en général le souhait du législateur ou du juge de protéger le citoyen lorsque la situation l'exige, en dépit des difficultés intrinsèques de mise en application liées au caractère transfrontalier de la situation, et d'appliquer ces règles en pratique afin de s'assurer que le but poursuivi est atteint.

Au niveau du droit de l'UE, plusieurs exemples illustrent une telle recherche de cohérence.

En matière de droit de la concurrence, la Commission européenne peut prendre des décisions qui touchent des sociétés établies en dehors de l'UE dans leurs activités sur le territoire de l'Union. À titre d'exemple, citons la récente décision de la Commission[8] de faire obstacle à la fusion[9] proposée de deux sociétés américaines : General Electric et Honeywell. Cette décision de juillet 2001 stipule (article premier) qu'une fusion des deux sociétés donnerait lieu à une « concentration incompatible avec le Marché commun ». La Commission a établi que les deux sociétés présentaient sur le territoire de l'Union un chiffre d'affaires total de plus de 250 millions d'euros, et a donc conclu que l'opération notifiée possédait une « dimension communautaire ».

---

[5] TGI Paris, ordonnance du référé du 20 novembre 2000
http://legal.edhec.com/DTIC/Decisions/Dec_responsabilite_0.htm

[6] AG München, jugement du 28 mai 1998 – 8340 Ds 465 Js 173158/95

[7] BGH, jugement du 12 décembre 2000, Az: 1 StR 184/00

[8] Décision du 3 juillet 2001 cas n° COMP/M2220 conformément à l'article 8(3) du règlement (CEE) n°4064/89, Concentration entre entreprises

[9] Au terme de l'accord en question, Honeywell était destinée à devenir une filiale à cent pour cent de General Electric.

La dimension extraterritoriale du droit communautaire est également perceptible dans le droit lié à la protection des consommateurs. L'article 12 de la directive[10] concernant la protection des consommateurs en matière de contrats à distance stipule qu'un consommateur bénéficie toujours de la protection octroyée par la directive même lorsqu'une disposition contractuelle définit le droit applicable, et que la loi du pays non-membre choisi offre une protection moins importante que celle de la loi européenne. C'est le cas lorsque le contrat présente un « lien étroit » avec un ou plusieurs États membres[11]. La notion de « lien étroit » est extraite de l'article 7 de la convention de Rome de 1980. Cet article énonce que les « règles obligatoires » d'un pays doivent être appliquées aux situations pour lesquelles la loi d'un autre État est applicable, lorsque cette situation présente un « lien étroit » avec le pays.

La jurisprudence nous fournit un exemple supplémentaire, qui applique un raisonnement similaire avec la directive[12] concernant les agents commerciaux indépendants. La Cour de Justice européenne a jugé[13] que, lorsqu'un agent commercial exerçant son activité sur le territoire communautaire est employé par un commettant établi en dehors de l'Union, ce commettant ne peut se soustraire aux obligations de la directive en vertu d'une disposition contractuelle stipulant que la loi d'un pays tiers est applicable à la relation commerciale. La Cour a décidé que le droit communautaire doit s'appliquer lorsque « la situation présente un lien étroit avec la Communauté ».

Le secteur des compagnies aériennes nous fournit un exemple supplémentaire, plus pratique. Le Conseil a élaboré un règlement intitulé « Code de conduite des SIR » (systèmes informatisés de réservation)[14]. Ce règlement (qui réglemente l'utilisation des systèmes SIR) s'applique « aux systèmes informatisés de réservation […] proposés et/ou utilisés sur le territoire de la Communauté, indépendamment du statut ou de la nationalité du vendeur du système, ou […] de l'implantation de l'unité centrale de traitement des données ». Par conséquent, si un système est accessible au sein de l'UE, même lorsque l'équipement central du système n'est pas situé dans l'UE (et que les données alimentent ce système via des terminaux situés au sein de l'UE ou d'une autre manière), le droit de l'UE s'applique automatiquement.

Par conséquent, l'examen de l'applicabilité du droit de l'UE aux cas de figure présentant une dimension extraterritoriale permet de conclure que des critères similaires sont appliqués de manière générale. Qu'il soit nécessaire que la relation présente une « dimension communautaire » ou un « lien étroit » avec la Communauté, dans certaines situations, la Cour de Justice européenne, le Parlement européen et le Conseil ainsi que la Commission européenne estiment juste d'imposer des règles communautaires à des entités non établies sur le territoire européen.

---

[10] Directive 97/7/CE

[11] L'article 6(2) de la directive 93/13 concernant les clauses abusives dans les contrats conclus avec les consommateurs et l'article 7(2) de la directive 99/44 sur certains aspects de la vente et des garanties des biens de consommation sont très similaires à l'article 12(2). Ils insistent tous deux sur l'application des lois de l'UE et utilisent tous deux le terme « lien étroit ».

[12] Directive 86/653/CEE

[13] Affaire C-381/98, Ingmar GB Ltd. et Eaton Leonard Technologies

[14] Code de conduite pour l'utilisation de systèmes informatisés de réservation (SIR) (version combinée des règlements du Conseil n°323/99 modifiant le règlement n°3089/93 modifiant le règlement n°2299/89)

Dans d'autres pays, par exemple aux Etats-Unis d'Amérique, les cours et lois appliquent des raisonnements similaires afin de soumettre des sites web étrangers aux règlements locaux : la loi américain e « Children's Online Privacy Protection Act » (COPPA) de 1998 s'applique également aux sites web étrangers qui collectent des informations personnelles des enfants établis sur le territoire des États-Unis[15]. Au terme de cette loi fédérale, l'opérateur d'un site web adressé à des enfants de moins de 13 ans (ou d'un site grand public dont l'opérateur collecte sciemment des informations auprès d'enfants) est obligé de respecter les dispositions du règlement COPPA. Cette loi définit les informations que l'opérateur doit fournir dans la déclaration de confidentialité, quand et comment un opérateur est obligé d'obtenir le consentement parental vérifiable et quelles sont les responsabilités de l'opérateur en matière de protection de la vie privée et de sécurité en ligne des enfants. Le point intéressant pour l'objectif recherché ici est que cette loi s'applique non spécifiquement aux sociétés américaines, mais également aux sociétés « établies sur Internet » et que donc, sur le plan de la juridiction de la loi, l'implantation physique du site web importe peu tant que le site en question est actif aux Etats-Unis. Lorsque c'est le cas, le site web sera soumis au lois américaines applicables.

Une étude du droit international suggère que les États ont tendance à utiliser plusieurs critères alternatifs pour déterminer de manière approfondie le champ d'application du droit national afin de couvrir le plus grand nombre possible de cas en vue d'offrir la plus large protection possible aux consommateurs et à l'industrie nationale. Cette tendance conduit inévitablement à appliquer plusieurs droits nationaux à une situation qui implique un élément transfrontalier. Des instruments juridiques internationaux tentent par conséquent de déterminer les critères pertinents de manière neutre et non-discriminatoire. Toutefois, la dernière tentative d'avancer sur un projet de convention relatif à la loi applicable aux contrats sous les auspices de la « Conférence de La Haye » a échoué car les pays n'ont pas pu convenir du critère décisif. Ceci nous permet d'identifier le nœud du problème lorsque nous abordons la question du droit applicable : un équilibre équitable doit être préservé entre les intérêts variés des pays concernés.

Dans ce contexte, notons que la directive de l'UE sur la protection des données comporte une clause explicite sur la loi applicable et indique un critère. Cette disposition n'est sans doute pas aisée à comprendre ou à manipuler, mais le fait que la directive de l'UE sur la protection des données aborde cette question essentielle est tout à l'avantage des personnes et des sociétés.

2. Article 4 de la directive 95/46/CE sur le droit applicable

L'article 4 de la directive est ici reproduit dans sa totalité : Droit national applicable

1. Chaque État membre applique les dispositions nationales qu'il arrête en vertu de la présente directive aux traitements de données à caractère personnel lorsque:

a) le traitement est effectué dans le cadre des activités d'un établissement du responsable du traitement sur le territoire de l'État membre; si un même responsable du traitement est établi sur le territoire de plusieurs États membres, il doit prendre les mesures

[15] 15 U.S.C. § 6502 (1)(A)(I), auquel fait référence Joel R.Reidenberg, voir note de bas de page n°5.

nécessaires pour assurer le respect, par chacun de ses établissements, des obligations prévues par le droit national applicable;

b) le responsable du traitement n'est pas établi sur le territoire de l'État membre mais en un lieu où sa loi nationale s'applique en vertu du droit international public;

c) le responsable du traitement n'est pas établi sur le territoire de la Communauté et recourt, à des fins de traitement de données à caractère personnel, à des moyens, automatisés ou non, situés sur le territoire dudit État membre, sauf si ces moyens ne sont utilisés qu'à des fins de transit sur le territoire de la Communauté.

2. Dans le cas visé au paragraphe 1 point c), le responsable du traitement doit désigner un représentant établi sur le territoire dudit État membre, sans préjudice d'actions qui pourraient être introduites contre le responsable du traitement lui-même.

Cet article traite des cas qui soulèvent la question du droit applicable pour des opérations de traitement de données à caractère personnel. Il s'agit des cas où un aspect au moins du traitement des données à caractère personnel dépasse les frontières de l'État membre. Par exemple : une société de marketing direct compile des listes de diffusion électronique sur des consommateurs établis dans plusieurs États membres et les utilise dans un État membre afin de procéder à l'envoi de publicités à ces consommateurs. Ou un site web américain place un cookie dans l'ordinateur de particuliers établis dans l'UE afin d'identifier le PC pour le site web et de combiner ces informations avec d'autres.

La directive fait la distinction générale entre, d'une part, des situations où les éléments transfrontaliers sont confinés aux États membres de l'UE ou à des territoires situés au-delà des frontières géographiques de l'Union européenne, mais où la loi d'un État membre s'applique en vertu du droit public international (le « cas diplomatique »)[16] et, de l'autre, des situations où le traitement implique des éléments qui dépassent des frontières de l'Union européenne[17].

En ce qui concerne les situations au sein de la Communauté, l'objectif de la directive est double : éviter des lacunes juridiques (où ne s'applique aucune législation en matière de protection des données) et éviter l'application double/multiple des lois nationales. Etant donné que la directive s'emploie à définir le droit applicable et définit dans cette optique un critère susceptible de résoudre chaque cas de figure, la directive elle-même remplit le rôle d'une « règle de conflit » et rend inutile tout recours à d'autres critères de droit international privé.

Pour trouver une réponse au problème, la directive utilise comme critère ou « facteur de lien » le « *lieu d'établissement du responsable du traitement* » ou en d'autres termes, le principe du pays d'origine habituellement appliqué sur le marché intérieur. Cela signifie concrètement :

---

[16] Cette affaire ne sera pas abordée dans ce document. Il faudrait également souligner que la directive, et donc l'article 4, s'appliquent au traitement par le secteur privé et le secteur public des données à caractère personnel soumises au droit communautaire. Le présent document de travail n'aborde toutefois pas la question de l'application de l'article 4 aux cas du secteur public.

[17] Cette distinction s'applique principalement au responsable du traitement. Il conviendrait de toute façon de mettre en évidence que le caractère applicable de la directive n'est nullement affecté par le fait qu'un responsable du traitement établi dans l'UE peut procéder au traitement en dehors de l'UE. Dans ce cas, la directive est encore d'application pour l'ensemble des opérations de traitement.

Lorsque le traitement est effectué dans le cadre des activités d'un établissement du responsable sur le territoire d'un État membre, les dispositions nationales de cet État membre en matière de protection des données s'appliquent au traitement.

Lorsque le même responsable du traitement est établi sur le territoire de plusieurs États membres, chacun des établissements doit respecter les obligations stipulées par les lois respectives des États membres concernés pour le traitement des données effectué dans le cadre de leurs activités. Ce n'est pas là une exception au principe du pays d'origine. Il s'agit simplement de son application la plus stricte : lorsque le responsable choisit d'avoir non un mais plusieurs établissements, il ne bénéficie pas de l'avantage selon lequel respecter une seule loi suffit pour toutes les activités exercées sur l'ensemble du marché intérieur. Ce responsable doit donc appliquer en parallèle les lois nationales correspondant à chacun des établissements. Le groupe de travail pourrait éventuellement traiter cet aspect ultérieurement.

L'application du principe du pays d'origine est justifiée dans un marché interne où les lois nationales en matière de protection des données offrent des protections équivalentes grâce à l'harmonisation des droits des personnes sur le plan de la protection des données et des obligations de l'industrie et d'autres responsables du traitement des données à caractère personnel. De cette manière, le principe du pays d'origine, qui constitue en quelque sorte une restriction du champ d'application des lois des États membres en matière de protection des données, ne comporte aucun effet contraire sur les droits et les intérêts de ses résidents ou de l'industrie. En effet, même si les lois des États membres ne sont pas applicables à tous les processus de traitement impliquant des sujets de données nationaux ou se déroulant sur le territoire national, le fait que la loi d'un autre État membre soit applicable présente un impact très limité, puisque les deux lois sont harmonisées par la directive et donc équivalentes. En outre, la coopération entre les autorités nationales de protection des données garantit la confiance, l'assurance et l'application effective du droit, quelle que soit la loi applicable. [18]

La situation est différente en ce qui concerne les opérations de traitement impliquant un responsable du traitement établi dans un pays tiers. Les lois nationales de ces pays tiers ne sont pas harmonisées ; la directive n'est pas applicable dans ces pays et la protection des personnes sur le plan du traitement de leurs données personnelles peut être par conséquent absente ou lacunaire. Le principe du pays d'origine, lié au lieu d'établissement du responsable du traitement, ne peut plus servir l'objectif de la détermination de la loi applicable. Il est nécessaire de passer à un autre facteur de lien. Le Parlement européen et le Conseil ont décidé de reprendre un des facteurs classiques de lien du droit international, à savoir le lien physique entre l'action et un système légal. Le législateur européen a choisi le pays sur lequel est situé l'équipement utilisé[19]. La directive s'applique par conséquent lorsque le responsable du traitement n'est pas établi sur le territoire de l'Union, mais décide de traiter à des fins spécifiques des données et utilise les moyens, automatisés ou non, situés sur le territoire d'un État membre.

---

[18] Voir article 28, paragraphe 6, première phrase de la directive 95/46/CE : « Indépendamment du droit national applicable au traitement en cause, chaque autorité de contrôle a compétence pour exercer, sur le territoire de l'État membre dont elle relève, les pouvoirs dont elle est investie conformément au paragraphe 3. », et la dernière phrase du même paragraphe sur leur obligation de coopérer.

[19] Ce n'est pas le cas lorsque l'équipement est utilisé uniquement pour assurer le transit des données sur le territoire de la Communauté.

L'objectif de cette disposition de l'article 4 paragraphe 1 lit. c) de la directive 95/46/CE est le suivant : éviter qu'une personne ne soit pas protégée lors d'un traitement effectué dans son pays pour la seule raison que le responsable du traitement n'est pas établi sur le territoire de la Communauté. Pour la simple raison, par exemple, que le responsable du traitement n'a, en principe, rien à voir avec l'Union. Mais il est également possible que certains responsables du traitement choisissent de s'établir hors de l'UE pour contourner l'application de la loi européenne.

Soulignons qu'il n'est pas nécessaire que la personne soit citoyen européen, qu'elle soit physiquement présente dans l'UE ou qu'elle y réside. La directive ne fait pas de distinction sur la base de la nationalité ou de la localisation parce qu'elle harmonise les lois des États membres qui traitent des droits fondamentaux octroyés à tous les êtres humains, quelle que soit leur nationalité. Ainsi, dans les cas qui seront discutés ci-après, la personne pourrait être un citoyen américain ou chinois. En termes d'application du droit européen en matière de protection des données, cette personne sera protégée de la même manière qu'un citoyen de l'UE. C'est la localisation des moyens de traitement utilisés qui compte.

La décision du législateur communautaire de soumettre à sa loi sur la protection des données le traitement qui utilise des moyens localisés dans l'UE reflète donc son souhait sincère de protéger les personnes sur son propre territoire. Au niveau international, il est reconnu que les États sont en mesure d'offrir une telle protection. L'article XIV de l'AGCS permet de formuler des exceptions aux règles du libre échange en vue de protéger les personnes, leur droit à la vie privée et à la protection des données, et de mettre en application cette loi.

La section suivante explique les termes pertinents pour déterminer le droit applicable :

2.1 Établissement

La notion d'établissement est pertinente à l'article 4 (1) c de la directive au sens où le responsable du traitement n'est pas établi sur le territoire communautaire . Le lieu d'établissement d'un responsable du traitement implique l'exercice effectif et réel d'une activité au travers d'accords stables et doit être déterminé conformément à la jurisprudence de la Cour de justice européenne . Selon la Cour, le concept d'établissement implique l'exercice réel d'une activité dans un lieu d'établissement fixe pour une période indéterminée[20]. L'exigence est également remplie si la société est constituée pour une période donnée.

Le lieu d'établissement d'une société qui fournit des services par le biais d'un site Internet n'est pas le lieu où est située la technologie qui supporte son site web ni le lieu d'accès au site web ma is le lieu où elle exerce son activité[21]. Exemple : une société de marketing direct est enregistrée à Londres et y développe des campagnes pour toute l'Europe. L'utilisation de serveurs web à Berlin et à Paris ne change rien au fait qu'elle est établie à Londres.

[20] Cas C-221/89 Factortame [1991] ECR I-3905 §20

[21] Directive 2000/31/CE, considérant n°19.

2.2 Le responsable du traitement

Le *responsable du traitement* est un concept général extrait de la directive, définissant la personne physique ou morale qui, seule ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel (article 2 (d) de la directive 95/46/CE). La définition est neutre en ce qui concerne le lieu d'établissement du responsable du traitement. Elle est exhaustive car tout traitement de données doit être attribué à un ou plusieurs responsables du traitement. Dans le contexte de l'article 4 (1) c de la directive, cela signifie qu'il doit y avoir un responsable du traitement quelque part au sens de la directive. Il semble également nécessaire que le traitement ait lieu dans le cadre d'une activité soumise au droit communautaire et donc à la directive. Le traitement exécuté par une personne physique dans le cadre d'une activité purement personnelle ou domestique n'entre pas dans le champ d'application de la directive.

Pour pouvoir faire appel à l'article 4 (1) c de la directive, le responsable du traitement doit « *faire usage de* moyens pour les finalités du traitement des données à caractère personnel » (et non uniquement pour en assurer le transit) situé sur le territoire d'un État membre[22]. Ceci suggère, semble-t-il, que le responsable du traitement est actif et qu'il nourrit des intentions particulières. Sa décision quant aux finalités et aux moyens du traitement comprend donc cet aspect.

2.3 Moyens

La directive ne propose pas de définition pour ce terme. Le Collins English dictionary définit « equipment » comme un ensemble d'outils ou d'appareils réunis dans un but spécifique.
Les PC, terminaux et serveurs, que l'on peut utiliser pour quasiment tout type de traitement de données, sont des exemples d'« equipment ».

La directive explique que l'*« equipment »* peut être automatisé ou non pour autant qu'il n'est pas utilisé uniquement à des fins de transit d'informations sur le territoire de la Communauté.

Les « moyens de transit » typiques sont les réseaux de télécommunications (dorsales, câbles, etc.) qui font partie de l'Internet et par lesquels les communications Internet voyagent du point d'expédition vers le point de destination..

2.4 Faire usage de moyens

Il est essentiel pour l'application de la loi en matière de protection des données dans l'UE de déterminer quand « le responsable du traitement fait usage de moyens pour les finalités du traitement des données à caractère personnel », cf. article 4 (1) (c) de la directive.

[22] Notons qu'il existe une différence entre le terme utilisé dans la version anglaise de l'article 4 (1) c « equipment » et les termes utilisés dans les autres versions de l'article 4 (1) c qui rappellent davantage le terme anglais « means ». La terminologie utilisée dans les autres versions de l'article 4 (1) c concordent avec la formulation de l'article 2 (d) définissant le responsable du traitement comme la personne qui décide des finalités et des « means » du traitement. Il faut cependant souligner que les précédentes versions anglaises de la directive (par exemple, dans la proposition d'amendement de 1992) utilisaient également le terme de « means », qui fut modifié au cours des négociations, assez tardivement, en « equipment », comme on peut le voir dans la position commune de mars 1995.

Le groupe de travail prônerait une approche prudente lorsqu'il s'agit d'appliquer à des cas concrets cette règle de la directive sur la protection des données. Son objectif est de garantir que les personnes bénéficient de la protection des lois nationales en matière de protection des données et de la supervision du traitement des données par les autorités nationales compétentes en la matière, lorsque le besoin s'en fait sentir, que cette protection est utile et que le degré d'applicabilité de la directive est correct, en gardant toutefois à l'esprit le cadre transfrontalier de la situation.

Ceci posé, le groupe de travail estime que toutes les interactions entre un utilisateur Internet établi dans l'UE et un site web hors UE n'aboutissent pas nécessairement à l'application de la loi européenne en matière de protection des données. Le groupe de travail a estimé que les moyens devraient être à la disposition du responsable lors du traitement de données à caractère personnel.

En outre, il n'est pas nécessaire que le responsable du traitement exerce un contrôle total sur les moyens. Le responsable du traitement dispose de ces moyens dans une mesure variable. Celle-ci est suffisante lorsque le responsable du traitement, en déterminant la manière avec laquelle ces moyens fonctionnent, prend les décisions adéquates concernant la nature des données et leur traitement. En d'autres termes, le responsable détermine quelles données sont collectées, stockées, transférées, modifiées, etc., de quelle manière et dans quel but.

Le groupe de travail considère que la notion de « faire usage » présuppose deux éléments : un certain type d'activité entreprise par le responsable et son intention de traiter des données à caractère personnel. Ceci n'implique pas que tout « usage » de « moyens » à l'intérieur de l'UE mène à l'application de la directive.

Toutefois, le pouvoir de disposition du responsable ne doit pas être confondu avec la propriété ou la possession de l'équipement, soit par le responsable du traitement, soit par la personne. En réalité, la directive n'attache aucune importance à la possession de l'équipement, quel qu'il soit.

L'interprétation présentée par le groupe de travail est totalement en accord avec la motivation du législateur européen à l'élaboration de la disposition de l'article 4 (1) c de la directive. Le considérant n°20 explique que « *l'établissement, dans un pays tiers, du responsable du traitement de données ne doit pas faire obstacle à la protection des personnes prévue par la présente directive; que, dans ce cas, il convient de soumettre les traitements de données effectués à la loi de l'État membre dans lequel des moyens utilisés pour le traitement de données en cause sont localisés et de prendre des garanties pour que les droits et obligations prévus par la présente directive soient effectivement respectés* ». C'est le corollaire nécessaire si l'on veut atteindre l'objectif plus large de la directive qui est « *d'éviter qu'une personne soit exclue de la protection qui lui est garantie en vertu de la présente directive* ».

3. Exemples pratiques

Le présent chapitre tend à traduire le conseil fourni par l'article 4 en solutions concrètes applicables dans des cas typiques. Un élément commun aux cas abordés ci-dessous est que l'utilisateur Internet ne sait pas forcément toujours si le site web qu'il va visiter et auquel il va fournir des données (consciemment ou non) est établi sur le territoire de l'UE ou en dehors. Les noms de domaine ne contenant aucun élément géographique ne

peuvent être localisés physiquement sans informations complémentaires. Même lorsqu'ils comportent des éléments géographiques, il n'est pas garanti que le site web est effectivement hébergé sur un serveur situé dans le pays indiqué.

Cas A : Cookies

Le responsable du traitement décide de collecter des données à caractère personnel au moyen d'un fichier texte (cookie) qui est placé sur le disque dur de l'ordinateur personnel de l'utilisateur, mais une copie peut très bien être conservée par le site web ou un tiers[23]. Lors d'une communication ultérieure, le site web accède aux informations enregistrées dans le cookie (et donc dans le PC de l'utilisateur) afin d'identifier le PC pour le responsable du traitement. Ce dernier a donc la possibilité de relier toutes les informations qu'il a récoltées au cours des sessions précédentes avec les informations qu'il collectera au cours des sessions suivantes. Il est ainsi possible de créer des profils utilisateur assez détaillés.

Les cookies sont une partie standard du trafic HTTP et peuvent donc être transportés sans entrave avec le trafic sur IP. Ils contiennent des informations sur le particulier que peut consulter le site web responsable du placement des cookies. Un cookie peut contenir toutes sortes d'informations que le site web désire y inclure : pages visitées, publicités cliquées, numéro d'identification de l'utilisateur, etc.[24]

Le SET-COOKIE est placé dans l'en-tête de réponse HTTP[25], en fait dans des hyperliens invisibles. Si une limite de durée est stipulée[26], le cookie sera stocké sur le disque dur de l'utilisateur Internet et renvoyé vers le site web d'origine du cookie (ou vers d'autres sites web du même sous-domaine) pendant la durée du cookie. Ce retour à l'expéditeur prendra la forme d'un champ COOKIE inclus dans le trafic Internet décrit ci-dessus et se produira sans aucune intervention de l'utilisateur.

Comme expliqué plus haut, le PC de l'utilisateur peut être considéré comme un « equipment » au sens de l'article 4 (1) c de la directive 95/46/CE. Il est établi sur le territoire d'un État membre. Le responsable a décidé d'utiliser cet équipement à des fins de traitement de données à caractère personnel et, comme expliqué dans les paragraphes

[23] Les *cookies* sont des données crées par un serveur web qui peuvent être stockées dans des fichiers texte pouvant être placés sur le disque dur de l'utilisateur d'Internet et dont une copie peut être conservée sur le site web. Ces fichiers sont une partie normalisée du trafic http, et peuvent donc être transportés sans entrave avec le trafic sur IP. Un *cookie* peut contenir un nombre unique (GUI, Global Unique Identifier) qui permet une meilleure personnalisation que les adresses IP dynamiques. Il permet au site web de garder une trace des habitudes et des préférences de l'utilisateur.
Les *cookies* contiennent une série d'URL (adresses) pour lesquelles ils sont valides. Lorsque le navigateur rencontre à nouveau ces URL, il envoie ces *cookies* spécifiques au serveur web.
Les *cookies* peuvent être de nature différente : ils peuvent être permanents mais aussi être programmés pour une durée limitée (les fameux « session *cookies* »).

[24] Voir l'ouvrage de Hagel III, J. et Singer, M. : « *Net Worth : the emerging role of the informediary in the race for customer information »,* Harvard Business School Press, 1999, p. 275

[25] Techniquement parlant, il est également possible d'exécuter des cookies en JavaScript ou dans les champs <META-HTTP EQUIV> situés dans le code HTML.

[26] Les cookies sans limite de durée préétablie sont appelés « session cookies » et disparaissent à la fermeture du navigateur ou au débranchement de la ou la prise.

précédents, plusieurs opérations techniques ont lieu sans que le sujet des données ait un pouvoir de contrôle. Le responsable du traitement dispose des moyens de l'utilisateur et ces moyens ne sont pas uniquement utilisés à des fins de transit sur le territoire de la Communauté.

Le groupe de travail est par conséquent d'avis que le droit national de l'État membre où est localisé cet ordinateur personnel s'applique à la question suivante : dans quelles conditions les données personnelles de l'utilisateur peuvent être collectées par le placement de cookies sur son disque dur ?

Comme le groupe de travail l'a souligné dans une précédente recommandation[27], l'utilisateur devrait être informé lorsqu'un logiciel Internet a l'intention d'envoyer, de stocker ou de réceptionner un cookie. Le message donné à l'utilisateur devrait spécifier, en termes clairs, quelles sont les informations qui seront stockées dans le cookie et à quelles finalités, ainsi que la période de validité du cookie. L'utilisateur doit avoir ensuite la possibilité d'accepter ou de rejeter l'envoi ou le stockage d'un cookie dans sa totalité. Il devrait être en mesure de déterminer les informations qui doivent être gardées ou supprimées du cookie en fonction de, par exemple, la période de validité du cookie, ou des sites web qui les envoient et les réceptionnent[28].

Cas B : JavaScripts, bannières et autres applications similaires

Les JavaScripts sont des applications logicielles envoyées par un site web sur l'ordinateur d'un utilisateur et qui permettent à des serveurs éloignés d'exécuter des applications sur le PC de l'utilisateur. En fonction du contenu du logiciel, les JavaScripts permettent d'afficher des informations sur une page web, mais aussi d'introduire des virus dans l'ordinateur (les fameux applets dangereux en Java) et/ou de collecter et traiter des informations à caractère personnel stockées dans l'ordinateur. Lorsque le responsable du traitement décide d'utiliser ces outils afin de collecter et de traiter des données à caractère personnel, il fait usage de l'équipement au sens de la directive et devra respecter les dispositions de la législation communautaire.

Une société de publicité, grâce à un accord avec les propriétaires d'un site (moteurs de recherche par exemple) donne l'ordre à un navigateur (et donc à l'ordinateur) du sujet des données de se connecter non seulement avec le moteur de recherche qu'il ou elle veut consulter, mais également avec le serveur de la société de publicité. De cette manière, le publicitaire a la possibilité non seulement d'afficher des bannières[29] à l'écran du sujet des

[27] Recommandation 1/99 WP 17 « Invisible and Automatic Processing of Personal Data on the Internet performed by Software and Hardware ».

[28] « Le respect de la vie privée sur Internet – Une approche européenne intégrée sur la protection des données en ligne », document de travail, WP 37 5063/00 fournit de plus amples informations sur la nature des cookies est sur la méthode à adopter pour les utiliser d'une manière optimale. Une description générale figure à la page 16 : « Les cookies sont des informations qui peuvent être stockées dans des fichiers texte écrits sur le disque dur de l'utilisateur Internet, et dont une copie peut être conservée sur le site web.».
La page 79 détaille les « tueurs de cookie » et traite tant de la réponse de l'industrie face aux problèmes de protection de la vie privée que soulèvent les cookies – c.-à-d. les mécanismes anti-cookies –, que de celle des activistes de la protection de la vie privée – c.-à-d. les programmes indépendants tels *cookie washer*, *cookie cutter* et *cookie master*.

[29] Les bannières sont de petites fenêtres graphiques apparaissant au-dessus ou intégrées dans le contenu du site web.

données, mais également d'enregistrer, au moyen du navigateur de l'utilisateur, l'adresse et les données de contenu que la personne envoie au moteur de recherche. Les publicités par bannières sont placées sur le site web demandé par un hyperlien invisible vers la société de publicité.[30]
Le responsable du traitement maîtrise dès lors, de l'endroit où il se trouve, le fonctionnement du navigateur pour le faire se connecter et transmettre des informations à un tiers.

En outre, pour que le client reçoive la publicité par bannière la plus pertinente, les publicitaires sur Internet créent des profils en utilisant des cookies envoyés via cet hyperlien invisible. Selon la configuration du navigateur, l'utilisateur peut prendre conscience qu'un cookie est installé et ainsi donner ou non son accord. Le profil du client est relié au numéro d'identification du cookie de la société de publicité, de manière à pouvoir être complété chaque fois que le client visite le site web lié par contrat au publicitaire. Ainsi, la collecte supplémentaire de données personnelles venant de l'utilisateur aura lieu via son ordinateur et sans son intervention chaque fois que l'utilisateur d'Internet visitera le site web contenant cette bannière.

La directive serait également applicable aux informations collectées par des logiciels espions ou *spyware*. Egalement appelés mouchards, ces logiciels sont secrètement installés dans le PC de l'utilisateur, par exemple à l'occasion du téléchargement de logiciels plus importants (permettant par ex. d'écouter de la musique), afin de renvoyer des informations à caractère personnel concernant le sujet des données (titres des musiques favorites du particulier par ex.). Ces logiciels sont également connus sous le nom d'applications E.T. : « car dès qu'ils sont installés dans l'ordinateur de l'utilisateur et qu'ils ont appris ce qu'ils voulaient savoir, ils font ce que fit le héros de Spielberg : téléphoner maison »[31] .
Ces nouvelles applications logicielles de suivi font souvent usage de JavaScript et d'autres techniques similaires et utilisent clairement les moyens du sujet de données (ordinateur, navigateur, disque dur, etc.) pour collecter des données et les renvoyer ailleurs. Puisque, par définition, ces technologies sont utilisées sans en informer l'utilisateur (le nom de « logiciel espion » ne laisse planer aucun doute), elles sont une forme de traitement de données invisible et illégitime.

*****

Le groupe de travail « Article 29 » est conscient du fait que, outre les deux exemples mentionnés dans les précédentes sections, il y a d'autres cas pratiques en rapport avec Internet susceptibles de soulever des difficultés d'interprétation, en partie à cause de la complexité technique de certains systèmes utilisés

---

[30] Pour plus d'informations, voir le chapitre 8, « Cybermarketing » de WP 37, « Le respect de la vie privée sur Internet ».

[31] Voir l'article de couverture du Time magazine de Adam COHEN, du 31 juillet 2000: « *How to protect your privacy: who's watching you? They're called E.T. programs. They spy on you and report back by "phoning home". Millions of people are unwittingly downloading them ». (Comment protéger votre vie privée ? Qui vous observe ? On les appelle les programmes E.T. Ils vous espionnent et mouchardent en « téléphonant maison ». Des millions de gens les téléchargent sans le savoir.)*

Le groupe de travail continuera à se pencher sur ces matières et pourrait aborder d'autres cas pratiques à la lumière des expériences nationales et des développements techniques susceptibles de jouer un rôle important à l'avenir.

Il aimerait souligner que, même dans les cas où l'application de la directive n'est pas tout à fait claire, le groupe s'emploie à poursuivre le dialogue avec les sociétés et les organisations de pays tiers qui rassemblent des données à caractère personnel dans l'Union Européenne afin de promouvoir des normes adéquates de protection des données pour les sujets des données.

4. Quelle est la signification pratique ?

a) Application des principes régissant la collecte de données à caractère personnel

Dans tous ces cas, l'application de la loi de l'UE en matière de protection des données signifie entre autres choses ce qui suit :

- Afin de garantir l'honnêteté et la légalité de la collecte de données à caractère personnel, le responsable du traitement doit définir clairement la finalité du traitement.

- Le responsable du traitement doit également garantir que les données sont adéquates, pertinentes et quantitativement en rapport avec le motif de la collecte.

- La collecte doit reposer sur un motif légitime (consentement sans ambiguïté, exécution d'un contrat, conformité à une obligation légale, dans l'exécution des intérêts légitimes du responsable du traitement, etc.) et le particulier a le droit d'accéder à ses données personnelles, ainsi que le droit de les corriger ou de les supprimer.

- Le particulier doit au moins être informé de l'identité du responsable du traitement et de son représentant, de la finalité de ses collectes, des destinataires et de ses droits[32].

- Un autre aspect important est la sécurité du traitement. Celle-ci pourrait obliger le responsable du traitement à appliquer dès le début de la collecte des mesures techniques et organisationnelles spécifiques destinées à protéger les données d'une destruction accidentelle ou illégale, d'une perte accidentelle, d'une modification, d'une divulgation ou d'un accès non autorisés, en particulier lorsque les données sont transmises au travers d'un réseau. De telles mesures devraient assurer un niveau de sécurité approprié en fonction des risques présents et de la nature des données.

- En ce qui concerne les données sensibles, des dispositions spécifiques, traitant en particulier d'exigences en matière de sécurité, réglementent leur collecte[33].

---

[32] L'article 10 de la directive stipule que des informations supplémentaires devraient être fournies lorsque cette manière de procéder est nécessaire pour garantir un traitement équitable du sujet des données. Dans le cas des cookies, le particulier devrait également avoir la possibilité d'accepter ou de refuser le placement d'un cookie. Il devrait également avoir la possibilité de définir quelles données il souhaite voir traitées ou non.

[33] Certains Etats membres pourraient exiger un contrôle préalable avant d'autoriser le traitement de données sensibles.

La recommandation 2/2001 du groupe de travail fournit de plus amples détails quant à la manière avec laquelle la directive sur la protection des données s'applique au traitement des données par des sites web ainsi que sur certaines exigences minimales applicables à la collecte en ligne de données à caractère personnel dans l'Union européenne[34].

b) Aspects de procédure

Conformément à l'article 4 (2) de la directive 95/46/CE, le responsable du traitement devrait également désigner un représentant établi sur le territoire de l'État membre où est situé l'équipement.

Les informations relatives aux identités du responsable du traitement et du représentant pourraient être facilement incluses dans la déclaration de confidentialité du site web ou dans les informations générales d'identification du responsable du site web, de telle manière que le responsable du traitement pour ce site web puisse être facilement identifié et contacté.

Il conviendrait de recommander le recours à un représentant unique, agissant pour le compte de plusieurs responsables du traitement, ou d'envisager d'autres solutions pragmatiques.

En ce qui concerne la notification de l'opération de traitement souhaitée (c.-à-d. la collecte) aux autorités nationales de protection des données, la directive prévoit plusieurs possibilités. Conformément à la première phrase de l'article 18 (1), le responsable du traitement ou son représentant doit avertir l'autorité de contrôle avant de procéder à n'importe quelle opération de traitement ou série d'opérations. L'article 19 (1) (a) stipule que la notification inclura entre autres éléments le nom et l'adresse du responsable du traitement et de son représentant.

Conformément à l'article 18 (2), deuxième alinéa, les États membres ne peuvent prévoir de simplification de la notification ou de dérogation à cette obligation que dans les deux cas suivants : pour les catégories d'opérations de traitement qui ne sont pas susceptibles de heurter les droits et libertés des sujets des données ou lorsque le responsable du traitement désigne un employé chargé des matières liées à la protection des données à caractère personnel, qui garantirait en toute indépendance de l'application interne de la législation en matière de protection des données[35].
Le groupe de travail est conscient du fait que l'application de ces dispositions pourrait poser des problèmes d'ordre pratique et serait disposé à y consacrer plus d'attention ultérieurement.

[34] Voir en substance la WP 43, recommandation 2/2001 concernant certaines exigences minimales pour la collecte en-ligne de données à caractère personnel dans l'Union européenne. Il conviendrait d'examiner si tous les éléments mentionnés dans la WP 43 vont être également applicables à la collecte en ligne de données au sein de l'UE par des responsables du traitement établis en dehors de l'UE.

[35] Pour les dispositions spécifiques de droit national relatives à la mise en œuvre de cet article de la directive, consulter : http://europa.eu.int/comm/internal_market/en/dataprot/law/impl.htm.

c) Mise en application

Il est évident que la mise en application de règles dans un contexte international n'est pas aussi facile que dans un seul pays donné. Le citoyen doit en être conscient (et il faut au besoin l'y aider). Néanmoins, il existe plusieurs possibilités que l'on peut développer en vue d'atteindre un niveau raisonnable de mise en application.

Pour atteindre un bon niveau d'application, nous devrions en premier lieu faire prendre conscience aux organisations européennes et internationales des exigences de la directive en matière de collecte des données dans l'Union européenne. La diffusion la plus large de cette recommandation n'est qu'une première étape. Le respect de la directive impliquerait également des solutions technologiques, fournissant une structure préétablie pour la collecte de données à caractère personnel, qui intégrerait les exigences décrites dans les outils logiciels utilisés pour la collecte de données à caractère personnel. Le groupe de travail a déjà fait référence à la possibilité d'imaginer des procédures d'autorisation de produit, qui incluraient un contrôle du respect des exigences légales en matière de protection des données à caractère personnel. Un système européen de labels/sceaux Internet, ouvert également à des sites web non-européens, pourrait être la pierre angulaire d'une telle action.

En outre, dans un cas concret, un particulier vivant dans l'Union Européenne connaissant des problèmes avec un site web non européen pourrait soumettre son cas à l'autorité nationale compétente en matière de contrôle de la protection des données. Cette autorité déterminerait si la directive ou la loi nationale en matière de protection des données est d'application. Si tel est le cas, cette autorité pourrait établir des contacts avec le site web étranger en vue de résoudre le problème. Si un cas est porté devant un tribunal dans un Etat membre où le particulier réside, ce tribunal décidera s'il peut exercer sa juridiction sur le cas en question (ce qui, selon le droit international de procédure, pourrait être le cas puisque la partie la plus concernée est le particulier vivant sur le même territoire que le tribunal). Si le tribunal peut exercer sa juridiction, il applique l'article 4 de la directive 95/46/CE ou la loi nationale concernée en la transposant, et peut ainsi démontrer que le site web étranger traitait les données personnelles de l'individu de manière illégale et malhonnête. Bien des pays tiers vont déjà permettre la reconnaissance et la mise en application du jugement. Même s'ils ne le font pas, certains exemples montrent que des sites web ont néanmoins dû se plier à tel jugement et adapter leur mode de traitement de données afin d'établir de bonnes pratiques et de maintenir une bonne image commerciale.

Dans les pays tiers où les règles de protection des données et les autorités de contrôles sont bien établies, la mise en application est évidemment moins problématique.

5. Conclusions

- Le groupe de travail « article 29 » sur la protection des données estime que l'interprétation des lois nationales telle qu'elle figure dans le présent document de travail présenterait des avantages considérables dans l'optique de concrétiser la sécurité légale des sites web établis en dehors de l'Union européenne. Le groupe de travail est convaincu qu'un niveau élevé de protection des particuliers ne peut être assuré que si les sites web établis en dehors de l'Union mais qui utilisent des équipements situés sur le territoire communautaire (cf. plus haut) respectent les garanties pour le traitement des données à caractère personnel, en particulier la

collecte et les droits des individus reconnus au niveau européen et applicables de toute manière à tous les sites web établis dans l'Union européenne.

- Le groupe de travail « article 29 » sur la protection des données considère que le développement d'un programme pour la promotion de règles européennes pragmatiques de protection des données aiderait également les responsables du traitement de pays tiers à mieux comprendre, mettre en pratique et démontrer le respect de la vie privée. Un système européen de labels/sceaux web, ouvert également à des sites web non-européens, pourrait être la pierre triangulaire d'une telle action.

- Le groupe de travail « article 29 » sur la protection des données invite la Commission à tenir compte du présent document dans ses travaux ultérieurs.

Fait à Bruxelles le 30 mai 2002

Pour le groupe de travail

Le Président

Stefano RODOTA